Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Privacy Investigation:

The Toronto Police Service's use of Mobile Licence Plate Recognition Technology to find stolen vehicles

April 29, 2003

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Web site: www.ipc.on.ca

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC Web site.

Table of Contents

Introduction 1

Background 1

Description of the MLPR Pilot Project 2

Issues Arising from the Investigation 4

Results of the Investigation 5

Issue A: Do the licence plate numbers collected by the police qualify as "personal information," as defined in section 2(1) of the *Act*? 5

Issue B: Are the police collecting licence plate numbers in compliance with section 28(2) of the *Act*? 6

Issue C: Are the police using licence plate numbers in compliance with section 31 of the *Act*? 6

Issue D: Are the police disclosing licence plate numbers to AutoVu Technologies in compliance with section 32 of the *Act*? 7

Other Matters 9

Using the MLPR System for Parking Enforcement 9

Summary of Conclusions 11

Summary of Recommendations 12

Introduction

Background

In late January 2003, a reporter from *The Toronto Star* contacted the Office of the Information and Privacy Commissioner/Ontario (IPC) to seek the Commissioner's views about a new technology being tested by the Toronto Police Service (the police) called the Mobile Licence Plate Recognition (MLPR) system. The police's three-month MLPR pilot project involves using a video camera system mounted on the top of a police car (the "street sweeper") that scans the licence plate numbers of parked cars and compares them to a "hot list" of stolen vehicles.

Although the street sweeper is currently being used only to find stolen vehicles, the newspaper reported that the MLPR system could also be linked with global positioning system (GPS) technology to enforce parking bylaws. A parking control officer could use the GPS-configured version of the MLPR system to scan the licence plate numbers of parked vehicles and also record the location, date and time these vehicles were parked on a street. When the parking control officer later returns to the same street and scans the licence plate numbers of parked vehicles, the system would buzz if a vehicle has been parked longer than the permitted time, and a ticket may be issued.

Shortly after being interviewed by the *Star*, the Commissioner decided to launch a privacy investigation into police use of the MLPR technology. The IPC received a complaint from a member of the public, who expressed concern about "arbitrary surveillance" by the police and alleged that the MLPR system violates the unreasonable search and seizure section of the Canadian Charter of Rights and Freedoms. The IPC also received e-mail correspondence from another member of the public who urged the Commissioner not to investigate the police's use of the MLPR system because "[a] safer Ontario means some sacrifices in privacy."

The scope of this investigation deals primarily with the use by the police of the MLPR system to track down stolen vehicles. Specifically, the investigation looked at whether the police are acting in compliance with the *Municipal Freedom of Information and Protection of Privacy Act*. The police service has not yet made a decision as to whether it will use the GPS-configured version of the system for detecting parking violations, so this issue is not yet ripe for investigation. However, in the "Other Matters" section of this report, the IPC offers some recommendations to the police service in the event that it chooses to test or implement the GPS-configured version of the MLPR system at some point in the future.

During the course of the investigation, the IPC held meetings with the police and the two private-sector entities involved in the pilot project: AutoVu Technologies and the Insurance Bureau of Canada (IBC). The IPC also took a ride in the street sweeper car to see how the MLPR system works in practice. Although the IPC does not have jurisdiction over the private sector (i.e., AutoVu Technologies and the IBC), all of the parties involved in the pilot project were open and transparent about the use of the MLPR system and fully co-operated with our requests for information, for which we are grateful.

Description of the MLPR Pilot Project

The MLPR system pilot project commenced on January 13, 2003 and ran for three months. The purpose of the project was to assess whether the MLPR system can make the retrieval of stolen vehicles more efficient and to locate vehicles that have been reported stolen. Although the assessment phase of the project has ended, the police are continuing to use the street sweeper to find stolen vehicles.

The MLPR system was developed by AutoVu Technologies, a Montreal-based company that supplies licence plate recognition technology to both law enforcement agencies and the private sector. The IBC, a national trade association representing property and casualty insurance companies, is sponsoring the $100,000 pilot project. The police have signed a memorandum of understanding with the IBC but do not have a formal contract with AutoVu Technologies.

Vehicles are stolen for a variety of purposes, including joyriding and as a mode of transport in the commission of a crime. In addition, vehicles are the targets of organized crime groups, which may ship the vehicles to other countries. According to the IBC, vehicle theft costs the insurance industry in Canada approximately $600 million each year, which works out to $48 per policyholder.

The Toronto police's 322 parking enforcement officers recover about 1,100 vehicles annually. The MLPR system may enable the police to recover a greater number of stolen vehicles and to locate stolen vehicles more quickly. During the three-month pilot project, the use of the MLPR system in the street sweeper car enabled the police to locate 153 stolen vehicles, which would result in the recovery of at least 600 additional vehicles annually even if only one street sweeper car were used.

The efficient recovery of stolen vehicles has potential benefits for both the insurance industry and auto insurance policyholders. Insurance companies have a 30-day window before they must pay a policyholder for the replacement cost of a stolen vehicle. Consequently, if more vehicles are recovered within the 30-day timeframe and returned to their owners, this reduces the costs to the insurance industry, which may also result in lower premiums for policyholders. The quick recovery of stolen vehicles may also benefit public safety because it lessens the chance that a criminal will reuse a vehicle to commit criminal acts.

The street sweeper car, which is operated by officers from the police parking enforcement unit, is taken out for two eight-hour shifts per day. It has two video cameras in tubes mounted on its roof, which are angled down to enable them to scan the licence plate numbers of parked vehicles as the street sweeper slowly moves along a street or in a municipal parking lot. The MLPR system can scan up to 1,000 licence plate numbers per hour. Each licence plate number is transmitted to an onboard computer and immediately compared to the database of stolen vehicles, which is stored on the hard drive of the computer.

The stolen vehicle database is extracted from CPIC (Canadian Police Information Centre), a national computer-based information system administered by the Royal Canadian Mounted Police (RCMP). The RCMP makes the stolen vehicle database available to law enforcement clients, including the Toronto Police Service. This database contains detailed information about

vehicles that have been reported stolen, including their licence plate number, vehicle identification number (VIN), make, model, colour and year.

As a Toronto Police Service officer drives down a street or in a municipal parking lot, the scanned licence plate number of each vehicle is displayed on the screen of the street sweeper's onboard computer. If the system detects a potential match to a stolen vehicle, the computer beeps to alert the officer, who then stops and visually scrutinizes the licence plate number of the parked vehicle and compares it to a list of stolen vehicle licence plate numbers that pop up along the bottom of the computer's display terminal. (In some cases, one or more characters on the licence plate may be obscured by mud or snow. Consequently, the system provides a list of stolen car licence plate numbers that are close to the plate number of the parked vehicle.)

If the officer finds that the licence plate number does not match any stolen vehicle plate numbers, he or she presses "reject" and continues on. However, if the officer finds that the plate number of the parked car matches the plate number of a stolen vehicle, he or she presses "enforce," which saves an image of the licence plate number on the hard drive of the onboard computer.

The officer must then contact an operator in the police radio room, who checks the updated CPIC database to determine whether the vehicle is still reported stolen. If the radio room operator confirms the stolen status of the vehicle, the officer manually records the vehicle's licence plate number, VIN, description, and location in a handwritten log. The police service's standard procedure for handling retrieved vehicles then kicks in, which includes towing the vehicle to a police pound.

The hard drive in the street sweeper's onboard computer has the capacity to retain approximately 72 hours worth of scanned licence plate numbers. Consequently, whenever the parking enforcement unit officer scans a licence plate number, this new scan overwrites any existing scan that is 72 hours old. In other words, the MLPR system is configured to automatically destroy all scanned licence plate numbers on the hard drive after 72 hours.

The police do not have access to the scans retained in the system because the hard drive is password-protected and the data is encrypted by AutoVu. However, the police download the contents of the hard drive onto a zip disk on a daily basis. This zip disk, which is sent to AutoVu once a week, includes an alphabetical string of all licence plates scanned during that week and the images of any licence plates that produced a hit when they were matched against the stolen vehicle database. The alphabetical string of licence plate numbers does not include the jurisdiction (e.g., Ontario) that appears on the top of the plate. However, both the licence plate number and jurisdiction are visible on the images of licence plates that are saved on the hard drive after producing a hit with the stolen vehicle database.

AutoVu Technologies requires this information to analyze whether the MLPR system is making the retrieval of stolen vehicles more efficient and to ensure that the MLPR equipment is properly scanning licence plate numbers and otherwise functioning properly. After AutoVu has analyzed the data supplied by the police, it erases the data on the zip disk and sends the disk back to the police's parking enforcement unit.

Issues Arising from the Investigation

We recognize that the police service's use of the MLPR system has potential benefits for law enforcement, the insurance industry and auto insurance policyholders; these benefits must be balanced against the privacy rights of the public. In particular, the police must comply with the privacy-protection rules in Part II of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

During the course of the investigation, the IPC identified the following four issues:

(A) Do the licence plate numbers collected by the police qualify as "personal information," as defined in section 2(1) of the *Act*?

(B) Are the police collecting licence plate numbers in compliance with section 28(2) of the *Act*?

(C) Are the police using licence plate numbers in compliance with section 31 of the *Act*?

(D) Are the police disclosing licence plate numbers to AutoVu Technologies in compliance with section 32 of the *Act*?

Results of the Investigation

Issue A: Do the licence plate numbers collected by the police qualify as "personal information," as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part, that "personal information" means recorded information about an identifiable individual, including:

> (c) any identifying number, symbol or other particular assigned to the individual ...

The IPC has established in at least one order (M-336) that a licence plate number is personal information. For the purposes of this investigation, the IPC reviewed the *Highway Traffic Act* and information available on the Ministry of Transportation's (MTO) Web site, which show that:

- Individuals retain their licence plate numbers when selling their motor vehicles;
- The seller can put his or her plates on a new vehicle, if he or she purchases one;
- An individual is supposed to surrender his or her plate when leaving to reside in a different province or country.

These facts establish that a licence plate number is clearly an "identifying number, symbol or other particular assigned to the individual." In some circumstances, a licence plate number may be assigned to a company, which means that it may not be an identifying number assigned to an individual. However, the vast majority of vehicle licence plate numbers scanned by the street sweeper car using the MLPR system would almost certainly be assigned to individuals.

The first part of the definition of personal information also stipulates that the information at issue must be "recorded information about an identifiable individual." Under section 2(1) of the *Act*, a "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, including a photograph.

The licence plate numbers at issue in this investigation are indisputably "recorded information." All scanned licence plate numbers are electronically saved on the hard drive of the street sweeper's onboard computer. While these scans only record the licence plate number and not the jurisdiction that runs across the top of the plate, the vast majority of licence plates scanned by the street sweeper are Ontario plates. The images of licence plates that produce a match with the stolen vehicle database are also downloaded to the hard drive. Both the plate number and jurisdiction are visible on these images.

The test for whether information is "about an identifiable individual" is whether there is a reasonable expectation that the individual can be identified from the information. The Toronto Police Service has a variety of tools for identifying the individual to whom a licence plate number has been assigned. For example, the police can obtain the name of the individual to whom a licence plate has been assigned by accessing MTO's Vehicle Registration Database. In short, it is reasonable to expect that the police can identify an individual based on a licence plate number. Consequently, a licence plate number is clearly information "about an identifiable individual."

Conclusion: The licence plate numbers collected by the police are "personal information" as defined in section 2(1) of the *Act*.

Issue B: Are the police collecting licence plate numbers in compliance with section 28(2) of the *Act*?

Section 28(2) of the *Act* prohibits the collection of personal information unless the collection is:

- expressly authorized by statute;
- used for the purposes of law enforcement; or
- necessary to the proper administration of a lawfully authorized activity.

The definition of law enforcement in section 2(1) of the *Act* includes "policing." The parking enforcement unit officers who are scanning licence plate numbers and comparing them against a database of stolen vehicles, are clearly engaging in "policing." Although the police are compiling licence plate numbers through the use of the MLPR system for the purpose of assessing whether the system can make the retrieval of stolen vehicles more efficient, they are also obtaining licence plate numbers for the purpose of locating vehicles that have been reported stolen. Consequently, the police's collection of licence plate numbers is used for the purpose of law enforcement, which is permitted under section 28(2) of the *Act*.

Conclusion: The police are collecting licence plate numbers in compliance with section 28(2) of the *Act*.

Issue C: Are the police using licence plate numbers in compliance with section 31 of the *Act*?

Section 31 of the *Act* sets out the circumstances under which an institution may use personal information. Subsection 31(b) states that an institution shall not use personal information in its custody and control except for the purpose for which it was obtained or compiled or for a consistent purpose.

The parking enforcement unit officers who drive the Street Sweeper obtain or compile licence plate numbers through the use of the MLPR system. As noted in Issue B, the police are obtaining licence plate numbers through the use of the MLPR system for the purpose of assessing whether the system can make the retrieval of stolen vehicles more efficient. They are also obtaining licence plate numbers for the purpose of locating vehicles that have been reported stolen.

After an officer obtains a licence plate number through the MLPR scanning process, the plate number is then put to a specific use. The MLPR system automatically compares the plate number against the stolen vehicle database, which is stored on the hard drive of the Street Sweeper's onboard computer.

In other words, the police are using these licence plate numbers for the purpose of finding stolen vehicles. Consequently, they are using the licence plate numbers in their custody and control for the purpose for which this personal information was obtained or compiled, which is permitted under section 31 of the *Act*.

Conclusion: The police are using licence plate numbers in compliance with section 31 of the *Act*.

Issue D: Are the police disclosing licence plate numbers to AutoVu Technologies in compliance with section 32 of the *Act*?

Section 32 of the *Act* prohibits an institution from disclosing personal information in its custody or under its control except for the specific and limited circumstances set out in subsections (a) to (l). In particular, subsection 32(c) permits an institution to disclose personal information for the purpose for which it was obtained or compiled or for a consistent purpose.

During the course of our investigation, we found that the police download the contents of the street sweeper's computer hard drive onto a zip disk on a daily basis. This zip disk, which is sent to AutoVu once a week, includes an alphabetical string of all licence plate numbers scanned during that week and the images of any licence plates that produced a hit when they were matched against the stolen vehicle database. This constitutes a disclosure of personal information to AutoVu.

The alphabetical string of licence plate numbers does not include the jurisdiction (e.g., Ontario) that appears on the top of the plate. However, both the licence plate number and jurisdiction are visible on the images of any licence plates saved on the hard drive of the street sweeper's onboard computer after producing a hit with the stolen vehicle database.

Although the police are obtaining licence plate numbers for the purpose of locating vehicles that have been reported stolen, they are also obtaining licence plate numbers for the purpose of assessing whether the system can make the retrieval of stolen vehicles more efficient. AutoVu

requires the string of scanned licence plate numbers and the images of licence plates that produced a hit to analyze whether the MLPR system is making the police's retrieval of stolen vehicles more efficient. Consequently, the police are disclosing the licence plate numbers that are in their custody and control for the purpose for which this personal information was obtained or compiled, which is permitted under subsection 32(c) of the *Act*.

We would note that although the police signed a memorandum of understanding with the IBC, they do not have a similar contract with AutoVu Technologies. There is no evidence that AutoVu uses the licence plate numbers that it receives from the police for inappropriate purposes or that it discloses this information to third parties. For example, the company does not match the licence plate numbers to the names of the individuals to whom the plates have been assigned. Moreover, the police have informed the IPC that if they decide to expand the use of the MLPR system after the pilot project has concluded, it will likely be unnecessary to continue the practice of disclosing licence plate numbers on a zip disk to AutoVu.

Nevertheless, the IPC recommends that, in future projects, the police sign a contract with any private-sector entity not subject to the *Act* to which they disclose personal information. Such a contract should include strong privacy-protection clauses that prohibit the private-sector entity from misusing or inappropriately disclosing any personal information that it receives from the police. This would include a prohibition on matching the personal information with any other information about an individual that the private-sector entity has collected from other sources. In addition, a requirement that the private-sector entity's employees sign confidentiality agreements should be included.

Conclusion: The police are disclosing licence plate numbers to AutoVu Technologies in compliance with section 32 of the *Act*.

Other Matters

Using the MLPR System for Parking Enforcement

Although the Toronto police are currently using the MLPR technology only to find stolen vehicles, the system has the capacity to be linked with global positioning system (GPS) technology to enforce parking bylaws. GPS refers to a group of U.S. Department of Defense satellites that are constantly circling the earth. These satellites transmit power signals that allow anyone with a GPS receiver to determine his or her precise location on the earth. GPS technology is increasingly being used for a number of different purposes. For example, hikers and motorists can use GPS devices to keep from getting lost. Moreover, GPS technology is being built into cell phones to help emergency services find individuals who have called 911.

A parking control officer can use the GPS-configured MLPR system to scan the licence plate numbers of parked vehicles and record the precise location, date and time these vehicles were parked on a street. When the parking control officer later returns to the same street and scans the licence plate numbers of parked vehicles, the system will buzz if a vehicle has been parked in the same location longer than the permitted time, and a ticket may be issued. This system is already being used in a number of North American cities, including North Vancouver, San Diego and Salt Lake City. The system was also tested by the City of Ottawa in 2001.

The *Act* does not compel municipal institutions to consult with the IPC before implementing initiatives or pilot projects that may have privacy implications. However, section 46(a) of the *Act* allows the Commissioner to offer comment on the privacy protection implications of proposed programs of municipal institutions. We would suggest that consultation with our office is not only in accordance with the spirit and intent of the *Act* but more so, can assist institutions in ensuring that they are acting in compliance with the *Act*.

On numerous occasions, the IPC has urged both provincial and municipal institutions, including law enforcement agencies, to consult with this office before launching any initiatives or programs that may impinge on privacy (e.g., Investigation PC-010005-1). In particular, we encourage institutions to consult with us on:

- Proposed legislation (statutes, regulations, by-laws) that may have privacy protection implications;
- Proposed programs or projects that raise novel privacy issues (e.g., the use of new surveillance technologies);
- Proposed programs that are potentially controversial from a privacy perspective (e.g., the use of video surveillance in public places, the privatization of government programs).

We would like to distinguish the existing MLPR system that is used for locating stolen vehicles from the GPS-configured system that could be used to detect illegally parked vehicles. The use of the MLPR system to find stolen vehicles is in compliance with the *Act* and produces benefits (e.g., crime prevention, returning stolen property to citizens) that outweigh the minimal impact on privacy that results from the scanning of licence plate numbers. The benefits that would result from using the GPS-configured system (e.g., improving parking flows, increasing revenues) are, in our view, comparatively less important and yet pose a greater threat to privacy. When coupled with GPS technology, the police could use the MLPR system to collect a much greater wealth of potentially privacy-invasive personal information.

Consequently, the IPC would place any proposal to use the GPS-configured system under a high degree of scrutiny to ensure that the privacy rights of the public are fully protected. The IPC would oppose the police keeping records of the precise location, date and time that all vehicles were parked on a particular street. Specifically, it is important to ensure that the system would not be inadvertently used to track and record the movements of law-abiding citizens or used for any other secondary purposes unrelated to law enforcement.

If the Toronto police decide to test or implement the GPS-configured MLPR system at some point in the future, the IPC recommends that they first consult with this office to discuss the privacy implications of using this technology. The IPC also recommends that the police conduct a privacy impact assessment (PIA). A PIA is a process for determining whether new technologies, information systems, or proposed programs or policies meet basic privacy requirements. This process consists of developing an information flow map, applying a set of privacy questions to the information flow, identifying any privacy risks, and developing a solution to address these risks. Conducting a PIA can help law enforcement agencies to anticipate the public's privacy concerns and to generate confidence that these privacy concerns are being considered and addressed.

Summary of Conclusions

Our investigation has concluded that:

(A) The licence plate numbers collected by the police are "personal information" as defined in section 2(1) of the *Act*.

(B) The police are collecting licence plate numbers in compliance with section 28(2) of the *Act*.

(C) The police are using licence plate numbers in compliance with section 31 of the *Act*.

(D) The police are disclosing licence plate numbers to AutoVu Technologies in compliance with section 32 of the *Act*.

Summary of Recommendations

Although the IPC has concluded that the Toronto police's use of the MLPR technology to find stolen vehicles is in compliance with the *Act*, the IPC makes the following recommendations:

(1) In any future technology projects that involve the collection of personal information, the Toronto police should sign a contract with any private-sector entity not subject to the *Act* to which they disclose this personal information. Such a contract should include strong privacy-protection clauses that prohibit the private-sector entity from misusing or inappropriately disclosing any personal information that it receives from the police. This would include a prohibition on matching the personal information with any other information about an individual that the private-sector entity has collected from other sources. In addition, a requirement that the private-sector entity's employees sign confidentiality agreements should be included.

(2) If the Toronto police decide to test or implement the GPS-configured MLPR system at some point in the future, they should first consult with the IPC to discuss the privacy implications of using this technology. In addition, they should conduct a privacy impact assessment to determine whether this system meets basic privacy requirements.

Ann Cavoukian, Ph.D.
Commissioner

April 29, 2002
Date

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca